

DIGITAL SIGNATURE SYSTEM AND METHOD BASED ON HARD LATTICE PROBLEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to systems and methods for producing digital signatures based on the hardness of solving a worst-case lattice problem.

2. Description of the Related Art

Digital signatures are used for many applications, including verifying the identity of the sender of a message. Most digital signature schemes rely on the difficulty of factoring a large number obtained as a product of two large prime numbers, or on computing discrete logarithms.

Goldreich et al. proposed using lattice reduction problems as a basis for producing digital signatures in Advances in Cryptography - CRYPTO, Springer LNCS, 1294:112-131 (1997). A lattice is a collection of points in n-dimensional space which satisfy certain properties, including (1) zero is in the set; (2) if a, b are in the set, then $a+b, a-b$ are also in the set; (3) the lattice is generated by at least one finite basis, i.e., there exists a finite set (called a "basis") such that every point in the lattice is expressible as an integer linear combination of the elements in the basis. The "length" of a basis is the length of the longest vector in the basis. It happens that a

lattice typically can be defined using one of many bases, with the shortest basis being hard to find when the number "n" of dimensions becomes large.

Accordingly, the present invention recognizes that in a lattice-based digital signature scheme, an n-dimensional lattice can be generated that has a hard-to-find short basis, which is used as a sender's private key to sign a message by mapping the message to a point in the n-dimensional space. A recipient of the message can access a public key - the lattice with a relatively long basis - to verify the sender's identity by verifying the location of the message in the n-dimensional space. Unfortunately, the scheme disclosed by Goldreich et al., as admitted by Goldreich et al., might result in mapping two messages close together in the n-dimensional space, which would defeat the scheme as to those two messages because both messages would have the same digital signature.

In the present assignee's U.S. Patent No. 5,737,425 to Ajtai, incorporated herein by reference, an interactive message authentication system is disclosed which uses lattices. Although directed primarily to message authentication, the '425 patent discloses a method for deriving a lattice with a short basis. As recognized by the present invention, however, a digital signature system, unlike a message authentication system, must provide irrefutability of a signature, such that a recipient of a message can show a message to a third party to prove the identity of the signer of the message, a feature not generally required in message authentication systems. The requirement of irrefutability is particularly important in e-commerce applications. Moreover, the invention disclosed in Ajtai is interactive, which in the context of digital signatures

could render it susceptible to so-called "intruder in the middle" attacks. With the above recognitions in mind, the present invention has provided the inventive solutions disclosed below.

SUMMARY OF THE INVENTION

5 A computer-implemented method is disclosed for digitally signing data. The method includes generating a lattice \mathcal{L} having at least one short basis establishing a private key and at least one long basis establishing a public key. Further, the method includes mapping at least the message μ or a concatenation thereof to a message point "x" in n-dimensional space using a function "f". The function "f" is selected such that the possibility of mapping two messages close together in the space is infeasible. Using the short basis, a lattice point "y" of the lattice \mathcal{L} is found that is close to the message point "x".

10 In a preferred embodiment, at least the message point "x" and the lattice point "y" are returned as a digital signature. If desired, the function "f" can be randomized by concatenating the message μ with a random number ρ . Both the message μ and random number ρ are binary strings.

15 In one embodiment, the function "f" maps the message μ to a point on a grid. In this embodiment, the function "f" can be collision intractable, the collision intractability of which is derived from the hardness of lattice problems. In another embodiment, the function "f" is collision intractable. In still another embodiment, the function "f" maps at least the message to a point on an auxiliary lattice.

The present method can also include verifying a digital signature at a receiver computer at least in part by determining whether a difference between the lattice point "y" and the message point "x" is no more than a predetermined distance. The predetermined distance can be related to the number of dimensions in the lattice \mathcal{L} .

5 In another aspect, a computer program storage device includes a program of instructions for generating a digital signature for a message. The program of instructions in turn includes computer readable code means for mapping a message μ or a concatenation with a random string ρ to a message point "x" in n-dimensional space, with the message point "x" being a point of a grid or a point of an auxiliary lattice. Also, computer readable code means find a point "y" of a key lattice \mathcal{L} that is nearby the message point "x", and computer readable code means establish a digital signature, based at least on the points "x" and "y".

10 In still another aspect, a computer system for generating a digital signature of a message μ includes at least one sender computer. The sender computer includes logic for executing method steps that include mapping the message μ to a message point "x" at which it is not feasible to map any other message. Moreover, the logic of the sender computer finds a lattice point "y" that is relatively close to the message point "x", and then the logic transmits at least the message μ and the points "x" and "y". Further, the system includes at least one receiver computer that receives the message μ and points "x" and "y" and that executes logic including determining 20 whether a distance between the points "x" and "y" is related in a predetermined way

to a predetermined distance. Based thereon, it is determined whether the message μ has been properly signed.

5 In yet another aspect, a computer-implemented method for digitally signing data includes generating a lattice \mathcal{L} having at least one short basis and at least one long basis. The method also includes mapping at least the message μ or a concatenation thereof to a message point "x" in n-dimensional space. The message point "x" is an element of a set of spaced-apart points. Using the short basis, a lattice point "y" of the lattice \mathcal{L} is found that is close to the message point "x".

10 The details of the present invention, both as to its structure and operation, can best be understood in reference to the accompanying drawings, in which like reference numerals refer to like parts, and in which:

BRIEF DESCRIPTION OF THE DRAWINGS

15 Figure 1 is a block diagram of the present system;
Figure 2 is a flow chart of the logic used during generation of a lattice-based digital signature; and
Figure 3 is a flow chart of the logic for verifying the digital signature.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

20 Referring initially to Figure 1, a preferably non-interactive system for generating digital signatures based on lattice problems is shown, generally designated 10. Because the preferred system 10 is non-interactive, it is immune from so-called

"intruder in the middle" attacks. In the particular architecture shown, the system 10 includes a sender computer 12 that executes a software-implemented digital signature module 14 in accordance with the logic below to digitally sign messages. As shown in Figure 1, the sender computer 12 can send a message μ , a message point "x", a lattice point "y", and, if desired, a randomly generated number ρ in accordance with the disclosure below to a receiver computer 16. In turn, the receiver computer 16 executes a receiver module 18 to verify the signature.

It is to be understood that the logic disclosed herein may be executed by a processor as a series of computer-executable instructions. The instructions may be contained on a data storage device with a computer readable medium, such as a computer diskette. Or, the instructions may be stored on a DASD array, magnetic tape, conventional hard disk drive, electronic read-only memory, optical storage device, or other appropriate data storage device. In an illustrative embodiment of the invention, the computer-executable instructions may be lines of compiled C⁺⁺ compatible code.

In any case, the flow charts herein illustrate the structure of the modules of the present invention as embodied in computer program software. Those skilled in the art will appreciate that the flow charts illustrate the structures of computer program code elements including logic circuits on an integrated circuit, that function according to this invention. Manifestly, the invention is practiced in its essential embodiment by a machine component that renders the program code elements in a form that

instructs a digital processing apparatus (that is, a computer) to perform a sequence of function steps corresponding to those shown.

Figure 2 shows the logic of the digital signature module 14. The following notation is used for the below discussion. The notation that $x \in_R X$ means that the number "x" is chosen uniformly randomly from the set X. For a binary string x, the symbol $|x|$ denotes its length. For binary strings x, y, the symbol $x \circ y$ denotes their concatenation. All distances and norms are assumed to be Euclidean. For all integers $a, b > 0$, the notation Z_c^a is the set of all a-tuples of integers in the set $\{0, 1, \dots, c-1\}$. Similarly, Z_c^{axb} is the set of all matrices of "a" rows and "b" columns whose elements are integers in the set $\{0, 1, \dots, c-1\}$. For a set b_1, \dots, b_n of vectors, \mathcal{L} denotes the lattice of all integer linear combinations of b_1, \dots, b_n , with the vectors establishing a "basis" of the lattice \mathcal{L} . The length of a basis is the Euclidean norm of the length of the longest vector in the basis. Finally, the symbol $[x]$ denotes the integer portion of a number x.

With the above discussion in mind, commencing at block 20 in Figure 2, a lattice \mathcal{L} is generated that has a short basis and at least one long basis. The lattice \mathcal{L} preferably is generated using the principles set forth in the present assignee's U.S. Patent No. 5,737,425 to Ajtai. It is to be understood that the short basis of the lattice \mathcal{L} is generated along with the lattice, but that once the lattice is known, it is a difficult if not impossible problem to reverse engineer the short basis. The long basis of the lattice, accordingly, is published as the public key at block 22 and the short basis is maintained in secrecy as the private key of the present digital signature scheme.

In any case, in the preferred method for generating the lattice \mathcal{L} , set forth in the above-referenced patent, a variable "r" is selected that is sufficiently large such that the worst-case problems discussed in Ajtai, "Generating Hard Instances of Lattice Problems", Proc. 28th ACM Symposium on Theory of Computing, pages 99-108 (1996) and incorporated herein by reference, are hard. Moreover, variables c_{L1} and c_{L2} are selected such that it is infeasible to find vectors of length r^3 in n-dimensional lattices constructed in accordance with the above-referenced patent. Preferably, $c_{L2} \geq 9$ and $c_{L1} > c_{L2}$.

Letting $n = c_{L1}r(\log r)$, finding vectors of length r^3 is infeasible in the n-dimensional lattice \mathcal{L} that is created at block 20, assuming that certain worst-case lattice problems are hard in lattices of dimension n. Further, let q_L be the least odd integer satisfying $q_L \geq [r^{c_{L2}}]$, let $K = r^3$, and let $M = (nq_L)^{\frac{1}{2}}$. The preferred key lattice \mathcal{L} is a random lattice in $\Gamma'(n, M)$ as defined in the above-referenced patent, where an efficient construction of the lattice is also described that has a short basis generated along with it having a length of at most $K/3n$. In contrast, the public (long) basis preferably is at most of length M.

When the sender computer 12 desires to send a message μ , it enters a DO loop at block 24. Moving to block 26, the logic can, if desired, concatenate the message μ with a random string ρ . Then, proceeding to block 28, the message μ (or, more preferably, the concatenation $\mu \circ \rho$) is mapped to a message point "x" in n-dimensional space using a function "f" that is chosen such that it is infeasible that two messages would be mapped close to each other in space. "Close" is defined further

below in the context of the two grid-based mapping methods and one auxiliary lattice-based mapping method.

More specifically, for the grid-based methods, assume that A is an n -dimensional grid of size " d ", where the preferred $d = r^4$. Also, let $\ell = n^3q_L$, and let the above-mentioned function " f " be established by a mapping hash function $H: \{0,1\}^n \rightarrow \{0,1\}^\ell$. Further assume that the magnitude of the message is one-half n , i.e., that $|\mu| = n/2$. First, ρ is selected from the set $\{0,1\}^{n/2}$, and then the message point " x " is determined as an n -tuple of integers multiplied by " d " as follows: $x = H(\mu \circ \rho)d$. If the message point " x " as computed happens to be a point on the key lattice \mathcal{L} , the process above repeats with a new random string ρ .

In a first implementation of the grid-based method, the mapping function H is any hash function that satisfies the so-called Magic Hash Function condition that there exists an efficiently and publicly computable function that behaves like a random oracle. Some combination of hash functions such as Message Digest 5 (MD-5), "Sha", and "Snefru" are assumed to approximate the Magic Hash Function. Such a function is not collision-intractable.

In a second implementation of the grid-based method, the mapping function H is a collision-intractable function, preferably a lattice-based hash function, wherein c_{L1} and c_{L2} have the property that it is infeasible to find vectors of length r^3 in the lattice described in the above-referenced Ajtai publication. In this implementation, assume that q_H is the least odd integer satisfying $q_H \geq [r^{c_{L2}+4}]$. The output of the hash

function is n-tuples of integers in the set $\{0,1,\dots,q_{H-1}\}$. Further assume that $c_{H2} = c_{L2} + 4$, and $c_{H1} = c_{L1}$, so that $n = c_{H1}r\log(r) = c_{L1}r\log(r)$.

5

With the above definitions in mind, in the grid-based collision intractable embodiment, the mapping function $H \in_R Z^{rxn}_{q_H}$, and a variable m is a vector in Z_2^n that is an element of $\{0,1\}^n$. With this notation, $H(m) = Hm \bmod q_H \in Z_{q_H}^r$, the output of which function is an r-tuple of integers in Z_{q_H} . This output is interpreted as n integers of equal length, i.e., as a point in Z^n . As understood herein, it is computationally infeasible to find vectors of length "n" in the n-dimensional lattice of vectors $= x \in \{0,1\}^n$ such that $Hx = 0 \bmod q_H$. In other words, finding vectors of length $r^3 > n$ in the lattice of vectors defined by $x \in \{0,1\}^n$ is computationally infeasible. Moreover, it is to be appreciated that the collision intractability of the function "f" as implemented in the last of the above-disclosed grid-based mapping methods, and in the below-disclosed auxiliary lattice mapping method, is derived from the hardness of lattice problems.

10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995
1000
1005
1010
1015
1020
1025
1030
1035
1040
1045
1050
1055
1060
1065
1070
1075
1080
1085
1090
1095
1100
1105
1110
1115
1120
1125
1130
1135
1140
1145
1150
1155
1160
1165
1170
1175
1180
1185
1190
1195
1200
1205
1210
1215
1220
1225
1230
1235
1240
1245
1250
1255
1260
1265
1270
1275
1280
1285
1290
1295
1300
1305
1310
1315
1320
1325
1330
1335
1340
1345
1350
1355
1360
1365
1370
1375
1380
1385
1390
1395
1400
1405
1410
1415
1420
1425
1430
1435
1440
1445
1450
1455
1460
1465
1470
1475
1480
1485
1490
1495
1500
1505
1510
1515
1520
1525
1530
1535
1540
1545
1550
1555
1560
1565
1570
1575
1580
1585
1590
1595
1600
1605
1610
1615
1620
1625
1630
1635
1640
1645
1650
1655
1660
1665
1670
1675
1680
1685
1690
1695
1700
1705
1710
1715
1720
1725
1730
1735
1740
1745
1750
1755
1760
1765
1770
1775
1780
1785
1790
1795
1800
1805
1810
1815
1820
1825
1830
1835
1840
1845
1850
1855
1860
1865
1870
1875
1880
1885
1890
1895
1900
1905
1910
1915
1920
1925
1930
1935
1940
1945
1950
1955
1960
1965
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
2020
2025
2030
2035
2040
2045
2050
2055
2060
2065
2070
2075
2080
2085
2090
2095
2100
2105
2110
2115
2120
2125
2130
2135
2140
2145
2150
2155
2160
2165
2170
2175
2180
2185
2190
2195
2200
2205
2210
2215
2220
2225
2230
2235
2240
2245
2250
2255
2260
2265
2270
2275
2280
2285
2290
2295
2300
2305
2310
2315
2320
2325
2330
2335
2340
2345
2350
2355
2360
2365
2370
2375
2380
2385
2390
2395
2400
2405
2410
2415
2420
2425
2430
2435
2440
2445
2450
2455
2460
2465
2470
2475
2480
2485
2490
2495
2500
2505
2510
2515
2520
2525
2530
2535
2540
2545
2550
2555
2560
2565
2570
2575
2580
2585
2590
2595
2600
2605
2610
2615
2620
2625
2630
2635
2640
2645
2650
2655
2660
2665
2670
2675
2680
2685
2690
2695
2700
2705
2710
2715
2720
2725
2730
2735
2740
2745
2750
2755
2760
2765
2770
2775
2780
2785
2790
2795
2800
2805
2810
2815
2820
2825
2830
2835
2840
2845
2850
2855
2860
2865
2870
2875
2880
2885
2890
2895
2900
2905
2910
2915
2920
2925
2930
2935
2940
2945
2950
2955
2960
2965
2970
2975
2980
2985
2990
2995
3000
3005
3010
3015
3020
3025
3030
3035
3040
3045
3050
3055
3060
3065
3070
3075
3080
3085
3090
3095
3100
3105
3110
3115
3120
3125
3130
3135
3140
3145
3150
3155
3160
3165
3170
3175
3180
3185
3190
3195
3200
3205
3210
3215
3220
3225
3230
3235
3240
3245
3250
3255
3260
3265
3270
3275
3280
3285
3290
3295
3300
3305
3310
3315
3320
3325
3330
3335
3340
3345
3350
3355
3360
3365
3370
3375
3380
3385
3390
3395
3400
3405
3410
3415
3420
3425
3430
3435
3440
3445
3450
3455
3460
3465
3470
3475
3480
3485
3490
3495
3500
3505
3510
3515
3520
3525
3530
3535
3540
3545
3550
3555
3560
3565
3570
3575
3580
3585
3590
3595
3600
3605
3610
3615
3620
3625
3630
3635
3640
3645
3650
3655
3660
3665
3670
3675
3680
3685
3690
3695
3700
3705
3710
3715
3720
3725
3730
3735
3740
3745
3750
3755
3760
3765
3770
3775
3780
3785
3790
3795
3800
3805
3810
3815
3820
3825
3830
3835
3840
3845
3850
3855
3860
3865
3870
3875
3880
3885
3890
3895
3900
3905
3910
3915
3920
3925
3930
3935
3940
3945
3950
3955
3960
3965
3970
3975
3980
3985
3990
3995
4000
4005
4010
4015
4020
4025
4030
4035
4040
4045
4050
4055
4060
4065
4070
4075
4080
4085
4090
4095
4100
4105
4110
4115
4120
4125
4130
4135
4140
4145
4150
4155
4160
4165
4170
4175
4180
4185
4190
4195
4200
4205
4210
4215
4220
4225
4230
4235
4240
4245
4250
4255
4260
4265
4270
4275
4280
4285
4290
4295
4300
4305
4310
4315
4320
4325
4330
4335
4340
4345
4350
4355
4360
4365
4370
4375
4380
4385
4390
4395
4400
4405
4410
4415
4420
4425
4430
4435
4440
4445
4450
4455
4460
4465
4470
4475
4480
4485
4490
4495
4500
4505
4510
4515
4520
4525
4530
4535
4540
4545
4550
4555
4560
4565
4570
4575
4580
4585
4590
4595
4600
4605
4610
4615
4620
4625
4630
4635
4640
4645
4650
4655
4660
4665
4670
4675
4680
4685
4690
4695
4700
4705
4710
4715
4720
4725
4730
4735
4740
4745
4750
4755
4760
4765
4770
4775
4780
4785
4790
4795
4800
4805
4810
4815
4820
4825
4830
4835
4840
4845
4850
4855
4860
4865
4870
4875
4880
4885
4890
4895
4900
4905
4910
4915
4920
4925
4930
4935
4940
4945
4950
4955
4960
4965
4970
4975
4980
4985
4990
4995
5000
5005
5010
5015
5020
5025
5030
5035
5040
5045
5050
5055
5060
5065
5070
5075
5080
5085
5090
5095
5100
5105
5110
5115
5120
5125
5130
5135
5140
5145
5150
5155
5160
5165
5170
5175
5180
5185
5190
5195
5200
5205
5210
5215
5220
5225
5230
5235
5240
5245
5250
5255
5260
5265
5270
5275
5280
5285
5290
5295
5300
5305
5310
5315
5320
5325
5330
5335
5340
5345
5350
5355
5360
5365
5370
5375
5380
5385
5390
5395
5400
5405
5410
5415
5420
5425
5430
5435
5440
5445
5450
5455
5460
5465
5470
5475
5480
5485
5490
5495
5500
5505
5510
5515
5520
5525
5530
5535
5540
5545
5550
5555
5560
5565
5570
5575
5580
5585
5590
5595
5600
5605
5610
5615
5620
5625
5630
5635
5640
5645
5650
5655
5660
5665
5670
5675
5680
5685
5690
5695
5700
5705
5710
5715
5720
5725
5730
5735
5740
5745
5750
5755
5760
5765
5770
5775
5780
5785
5790
5795
5800
5805
5810
5815
5820
5825
5830
5835
5840
5845
5850
5855
5860
5865
5870
5875
5880
5885
5890
5895
5900
5905
5910
5915
5920
5925
5930
5935
5940
5945
5950
5955
5960
5965
5970
5975
5980
5985
5990
5995
6000
6005
6010
6015
6020
6025
6030
6035
6040
6045
6050
6055
6060
6065
6070
6075
6080
6085
6090
6095
6100
6105
6110
6115
6120
6125
6130
6135
6140
6145
6150
6155
6160
6165
6170
6175
6180
6185
6190
6195
6200
6205
6210
6215
6220
6225
6230
6235
6240
6245
6250
6255
6260
6265
6270
6275
6280
6285
6290
6295
6300
6305
6310
6315
6320
6325
6330
6335
6340
6345
6350
6355
6360
6365
6370
6375
6380
6385
6390
6395
6400
6405
6410
6415
6420
6425
6430
6435
6440
6445
6450
6455
6460
6465
6470
6475
6480
6485
6490
6495
6500
6505
6510
6515
6520
6525
6530
6535
6540
6545
6550
6555
6560
6565
6570
6575
6580
6585
6590
6595
6600
6605
6610
6615
6620
6625
6630
6635
6640
6645
6650
6655
6660
6665
6670
6675
6680
6685
6690
6695
6700
6705
6710
6715
6720
6725
6730
6735
6740
6745
6750
6755
6760
6765
6770
6775
6780
6785
6790
6795
6800
6805
6810
6815
6820
6825
6830
6835
6840
6845
6850
6855
6860
6865
6870
6875
6880
6885
6890
6895
6900
6905
6910
6915
6920
6925
6930
6935
6940
6945
6950
6955
6960
6965
6970
6975
6980
6985
6990
6995
7000
7005
7010
7015
7020
7025
7030
7035
7040
7045
7050
7055
7060
7065
7070
7075
7080
7085
7090
7095
7100
7105
7110
7115
7120
7125
7130
7135
7140
7145
7150
7155
7160
7165
7170
7175
7180
7185
7190
7195
7200
7205
7210
7215
7220
7225
7230
7235
7240
7245
7250
7255
7260
7265
7270
7275
7280
7285
7290
7295
7300
7305
7310
7315
7320
7325
7330
7335
7340
7345
7350
7355
7360
7365
7370
7375
7380
7385
7390
7395
7400
7405
7410
7415
7420
7425
7430
7435
7440
7445
7450
7455
7460
7465
7470
7475
7480
7485
7490
7495
7500
7505
7510
7515
7520
7525
7530
7535
7540
7545
7550
7555
7560
7565
7570
7575
7580
7585
7590
7595
7600
7605
7610
7615
7620
7625
7630
7635
7640
7645
7650
7655
7660
7665
7670
7675
7680
7685
7690
7695
7700
7705
7710
7715
7720
7725
7730
7735
7740
7745
7750
7755
7760
7765
7770
7775
7780
7785
7790
7795
7800
7805
7810
7815
7820
7825
7830
7835
7840
7845
7850
7855
7860
7865
7870
7875
7880
7885
7890
7895
7900
7905
7910
7915
7920
7925
7930
7935
7940
7945
7950
7955
7960
7965
7970
7975
7980
7985
7990
7995
8000
8005
8010
8015
8020
8025
8030
8035
8040
8045
8050
8055
8060
8065
8070
8075
8080
8085
8090
8095
8100
8105
8110
8115
8120
8125
8130
8135
8140
8145
8150
8155
8160
8165
8170
8175
8180
8185
8190
8195
8200
8205
8210
8215
8220
8225
8230
8235
8240
8245
8250
8255
8260
8265
8270
8275
8280
8285
8290
8295
8300
8305
8310
8315
8320
8325
8330
8335
8340
8345
8350
8355
8360
8365
8370
8375
8380
8385
8390
8395
8400
8405
8410
8415
8420
8425
8430
8435
8440
8445
8450
8455
8460
8465
8470
8475
8480
8485
8490
8495
8500
8505
8510
8515
8520
8525
8530
8535
8540
8545
8550
8555
8560
8565
8570
8575
8580
8585
8590
8595
8600
8605
8610
8615
8620
8625
8630
8635
8640
8645
8650
8655
8660
8665
8670
8675
8680
8685
8690
8695
8700
8705
8710
8715
8720
8725
8730
8735
8740
8745
8750
8755
8760
8765
8770
8775
8780
8785
8790
8795
8800
8805
8810
8815
8820
8825
8830
8835
8840
8845
8850
8855
8860
8865
8870
8875
8880
8885
8890
8895
8900
8905
8910
8915
8920
8925
8930
8935
8940
8945
8950
8955
8960
8965
8970
8975
8980
8985
8990
8995
9000
9005
9010
9015
9020
9025
9030
9035
9040
9045
9050
9055
9060
9065
9070
9075
9080
9085
9090
9095
9100
9105
9110
9115
9120
9125
9130
9135
9140
9145
9150
9155
9160
9165
9170
9175
9180
9185
9190
9195
9200
9205
9210
9215
9220
9225
9230
92

5

With the above definitions in mind, the message μ is concatenated, if desired, with the random string ρ as before at block 26, but then at block 28 the message point "x" is determined by multiplying the concatenation by the public matrix P . If the message point x is found to be an element of the key lattice \mathcal{L} , another random string ρ is selected and the process repeats.

In any case, it is to be appreciated that in the grid-based or lattice-based mapping schemes disclosed above, the message μ is mapped to a message point "x" that is a point on a grid or a lattice. In other words, in contrast to previous lattice mapping schemes the message point "x" must be an element of a set of points that are spaced apart from each other in n-dimensional space, such that no two points in the set are close together. This makes it infeasible that any two messages will be mapped to locations that are sufficiently close together so as to make a single signature apply to both.

1900-1901 1902-1903

20

Once the message has been mapped to the message point, the logic moves from block 28 to block 30, wherein a closest point "y" of the key lattice \mathcal{L} to the message point "x" is determined, using the (private) short basis of the key lattice \mathcal{L} . Specifically, using the short basis, a point $y \in \mathcal{L}$ is obtained such that $\|x-y\| \leq nK/(3n)$ (which, it will be recalled, $= r^3/3$) by writing x as a linear (possibly non-integral) combination of vectors in the short basis, each of which has a length of at most $K/(3n)$, and then rounding the coefficients to get $y \in \mathcal{L}$. Then, at block 32, the message μ , random string ρ (if used), message point "x", and closest lattice point "y"

are output for transmission of the message with lattice-based digital signature to the receiver computer 16.

Figure 3 shows that logic by which the receiver module 18 of the receiver computer 16 verifies the signature output at block 32. Commencing at block 34, the message μ , random string ρ (if used), message point "x", and closest lattice point "y" are received. Moving to block 36, it is verified, using the long basis, that the lattice point "y" is indeed a point on the key lattice \mathcal{L} . If desired, it can be further verified that $\mu \circ \rho \in \mathbb{Z}_2^n$. When a grid-based mapping method is employed, it can be further verified that $x = H(\mu \circ \rho)d$, whereas when an auxiliary lattice mapping method is used it can be verified that $x = P(\mu \circ \rho)$.

Moreover, using the long basis the receiver computer 16 moves to block 38 to verify that the message point "x" is indeed close to the lattice point "y". In a particularly preferred embodiment, this is done by verifying that $| | x-y | | \leq r^3/3$. More generally, at block 38 it is determined whether a difference between the lattice point "y" and the message point "x" is no more than a predetermined distance. If any test fails, it can be determined that the message μ has not been properly signed.

While the particular DIGITAL SIGNATURE SYSTEM AND METHOD BASED ON HARD LATTICE PROBLEM as herein shown and described in detail is fully capable of attaining the above-described objects of the invention, it is to be understood that it is the presently preferred embodiment of the present invention and is thus representative of the subject matter which is broadly contemplated by the present invention, that the scope of the present invention fully encompasses other

embodiments which may become obvious to those skilled in the art, and that the scope of the present invention is accordingly to be limited by nothing other than the appended claims, in which reference to an element in the singular is not intended to mean "one and only one" unless explicitly so stated, but rather "one or more". All structural and functional equivalents to the elements of the above-described preferred embodiment that are known or later come to be known to those of ordinary skill in the art are expressly incorporated herein by reference and are intended to be encompassed by the present claims. Moreover, it is not necessary for a device or method to address each and every problem sought to be solved by the present invention, for it to be encompassed by the present claims. Furthermore, no element, component, or method step in the present disclosure is intended to be dedicated to the public regardless of whether the element, component, or method step is explicitly recited in the claims. No claim element herein is to be construed under the provisions of 35 U.S.C. §112, sixth paragraph, unless the element is expressly recited using the phrase "means for".

WE CLAIM: